Please amend the claims as follows (this listing replaces all prior listings):

1. (currently amended) A method comprising:

detecting a possible security problem at a client location;

transmitting notice of the possible security problem across a network in real time to a home location remotely located from the client location;

determining at the home location an anomaly based on at least the possible security problem and on information sent to the home location from at least one other client location; and

transmitting notice of the anomaly in real time to the client location at which the possible security problem is detected.

2. (original) The method of claim 1 further comprising transmitting notice of the anomaly in real time to other client locations that may communicate with the home location over the network.

3. (original) The method of claim 1 further comprising notifying a firewall located between the client location and the home location about the anomaly.

4. (original) The method of claim 1 further comprising inspecting a packet that arrives at the client location to detect the possible security problem.

5. (original) The method of claim 1 in which the network includes a virtual private network.

6. (currently amended) The method of claim 1 in which the anomaly includes unauthorized access to the network.

7. (original) The method of claim 1 in which the anomaly includes unauthorized access of a resource accessible through the network.

8. (original) The method of claim 1 in which the anomaly includes unauthorized use of resources available through the network.

9. (currently amended) An article comprising:

a machine-readable medium which contains machine-executable instructions, the instructions causing a machine to:

detect a possible security problem at a client location;

transmit notice of the possible security problem across a network in real time to a home location remotely located from the client location;

determine at the home location an anomaly based on at least the possible security problem and on information sent to the home location from at least one other client location; and

transmit notice of the anomaly in real time to the client location at which the possible security problem is detected.

10. (original) The article of claim 9 further causing a machine to transmit notice of the anomaly in real time to other client locations that may communicate with the home location over the network

11. (original) The article of claim 9 further causing a machine to notify a firewall located between the client location and the home location about the anomaly.

12. (original) The article of claim 9 further causing a machine to inspect a packet that arrives at the client location to detect the possible security problem.

13. (original) The article of claim 9 in which the network includes a virtual private network.

14. (original) The article of claim 9 in which the anomaly includes unauthorized access to the network.

15. (original) The article of claim 9 in which the anomaly includes unauthorized access of a resource accessible through the network.

16. (original) The article of claim 9 in which the anomaly includes unauthorized use of resources available through the network.

17. (currently amended) A method comprising:

at a home location in a network, receiving from a remote client ~~location~~ an indication of a possible security problem at the client; and

determining in real time at the home location an existence of an anomaly based on at least the indication of the possible security problem and on information sent to the home location from at least one other remote client.

18. (original) The method of claim 17 further comprising transmitting notice of the existence of the anomaly in real time from the home location to the remote client location.

19. (currently amended) The method of claim 17 further comprising notice of the existence of the anomaly in real time from the home location to other remote client locations that ~~many~~ may communicate with the home location over the network.

20. (original) The method of claim 17 further comprising notifying, from the home location, a firewall located between the remote client location and the home location about the anomaly.

21. (original) The method of claim 17 further comprising transmitting information from the home location to the remote client location to help the remote client location identify possible security problems.

22. (original) The method of claim 17 further comprising determining the existence of the anomaly based on at least information regarding previous anomalies.

23. (cancelled) A method comprising:

detecting a possible security problem at a client location;

transmitting notice of the possible security problem across a network in real time to a home location remotely located from the client location; and

receiving in real time at the client location a notice from the home location indicating an existence of an anomaly based on at least the possible security problem.

24. (cancelled) The method of claim 23 further comprising inspecting a packet that arrives at the client location to detect the possible security problem.

25. (cancelled) The method of claim 23 further comprising receiving in real time at the client location a notice from the home location indicating an existence of a possible security problem detected by another client location that can communicate with the home location over the network.

26. (cancelled) An apparatus comprising:

a client terminal;

a first mechanism accessible by the client terminal and configured to detect a possible security problem at the client terminal;

a second mechanism accessible by the client terminal and configured to transmit notice of the possible security problem across a network in real time to a server remotely located from the client terminal; and

a third mechanism accessible by the client terminal and configured to receive updates from the server in real time regarding security problems that the first mechanism may use in detecting possible security problems.

27. (cancelled) The apparatus of claim 26 in which the first mechanism is also configured to monitor packets that arrive at the client terminal for the possible security problem.

28. (currently amended) An apparatus comprising:

a server;

a first mechanism accessible by the server ~~and configured~~ to determine an anomaly based on at least information from a client regarding a possible security problem and on information sent to the home location from at least one other client; and

a second mechanism accessible by the server and configured to transmit notice of the anomaly in real time over a network to the clients ~~client and to other client locations that may communicate with the server over the network~~.

29. (currently amended) The apparatus of claim 28 in which the first mechanism ~~is~~ also ~~configured to determine~~ determines the anomaly based on at least information regarding previously determined anomalies.

30. (currently amended) A system comprising:

a client terminal;

a server;

a first client mechanism accessible by the client terminal ~~and configured~~ to detect a possible security problem at the client terminal;

a second client mechanism accessible by the client terminal ~~and configured~~ to transmit notice of the possible security problem across a network in real time to a server remotely located from the client terminal;

a third client mechanism accessible by the client terminal ~~and configured~~ to receive updates from the server in real time regarding security problems that the first client mechanism may use in detecting possible security problems;

a first server mechanism accessible by the server ~~and configured~~ to determine an anomaly based on at least information from a client regarding a possible security problem and on information sent to the home location from at least one other client terminal; and

a second server mechanism accessible by the server ~~and configured~~ to transmit notice of the anomaly in real time over the network to the client terminal at which the possible security problem is detected.

31. (original) The system of claim 30 in which the first client mechanism is also configured to monitor packets that arrive at the client terminal for the possible security problem.

32. (original) The system of claim 30 in which the first server mechanism is also configured to determine the anomaly based on at least information regarding previously determined anomalies.

33. (original) The system of claim 30 in which the second server mechanism is also configured to transmit notice of the anomaly in real time to other client locations that may communicate with the server over the network.

34. (original) The system of claim 30 further comprising a firewall located between the client terminal and the server and configured to act as an intermediary for information flowing between the client terminal and the server.

35. (original) The system of claim 34 in which the firewall includes a corporate server.

36. (cancelled) A method comprising:

processing information relating to possible security problems associated with a private network at a home location to determine a security problem; and

modifying a monitoring agent included at each one of multiple clients to reflect the security problem, each one of the multiple clients capable of communicating the information to the home location.

37. (cancelled) The method of claim 36 further comprising performing the modifying in real time.

38. (cancelled) The method of claim 36 in which the multiple clients can communicate the information in real time.

39. (new) The method of claim 1 in which the information sent to the home location from the other client location comprises notice of a possible security problem at the other client location.

40. (new) A method comprising:

at a server, receiving from at least two remote clients indications of possible security problems at the clients; and

determining in real time at the server an existence of an anomaly based on the indications of the possible security problems from the at least two remote client locations.

41. (new) A method comprising:

detecting a possible security problem at a client location;

transmitting notice of the possible security problem across a network in real time to a home location remotely located from the client location;

determining at the home location an anomaly based on the possible security problem by searching for particular information in the anomaly, the particular information including at least one of a network address previously noted as a security problem, a particular query or command associated with a known intrusion pattern or technique, and a particular file name or file type associated with a known intrusion pattern or technique; and

transmitting notice of the anomaly in real time to the client location.

42. (new) A method comprising:

detecting a possible security problem at a client location;

transmitting notice of the possible security problem across a network in real time to a home location remotely located from the client location;

determining at the home location an anomaly by at least comparing the possible security problem with information previously logged at the home location; and

transmitting notice of the anomaly in real time to the client location.

43. (new) The method of claim 42 in which determining the anomaly comprises searching for non-standard access patterns.

44. (new) The method of claim 43 in which the non-standard access patterns comprise at least one of a login at an unexpected hour, a login from an unexpected location, and a login from an unexpected user.

45. (new) The apparatus of claim 28, further comprising at least one of a human immune mechanism to collect information on users, a complexity theory mechanism to store and perform complex analysis of anomaly trends, a statistics mechanism to compute and store records of anomalies, and a fingerprinting mechanism to check and store names and addresses associated with security problems.

46. (new) The apparatus of claim 28, further comprising a wide view mechanism to collect and maintain information regarding anomalies reported to the server by the clients.